HCFA/TennCare EDI Front Matter

November 2016 Version 3

Table of Contents

I. Introduction
- 1.01 Document Objective 1
- 1.02 HIPAA Companion Guides....1
- 1.03 TennCare Introduction 2
- 1.04 PPACA/ACA Section 1104 Overview 3
- 1.05 HIPAA Supported Transactions 3

II. Trading Partner Agreement and Supporting Documents and Supporting Documents
- 2.01 General Overview....4
- 2.02 TennCare Electronic Data Interchange Request Form 5
- 2.03 TennCare User Security Agreement 5
- 2.04 TennCare Remote Access Request Form 6
- 2.05 Additional Forms 6

III. EDI Services and Fees
- 3.01 EDI Services 6
- 3.02 Fees 7

IV. Technical Environment and Testing Considerations
- 4.01 TennCare Communications Requirements 7
- 4.02 File Encryption Procedures 8
- 4.03 File and Directory Naming Conventions 8
- 4.04 Multiple Transactions within a File....9
- 4.05 Size of Transmissions/Batches 9
- 4.06 Complete Transmission Check 10
- 4.07 Strategic National Implementation Process (SNIP) Test Types 10
- 4.08 Balancing Data Elements....11

V. Testing Procedures
- 5.01 Testing Requirements....11
- 5.02 Test Data....11

VI. Acknowledgment Processes
- 6.01 Overview of Acknowledgment Processes 12
- 6.02 TennCare Requirements 12
- 6.03 Rejected Transmissions and Transactions....12

Article I. Introduction

Section 1.01 Document Objective

This document provides information related to the HIPAA Transactions available from HCFA/TennCare EDI, establishment of Trading Partner relationships with HCFA/TennCare, set up and on-going fees associated with EDI services and types of available services. Tennessee Health Care Finance and Administration (HCFA) is the parent agent for TennCare which is the Medicaid program for the State of Tennessee. Hereafter within this document, HCFA/TennCare will be referred to as TennCare.

Section 1.02 HIPAA Companion Guides

TennCare Companion Guides (TCCGs) are compliant with the CORE standards being created from the CORE v5010 Master Companion Guide Template, and reviewed and approved by the Data Interchange Standards Association (DISA) after TennCare specific documentation had been added. TennCare Companion Guides can be made available upon request by any TennCare registered Trading Partner.

TCCGs are intended to be supplemental to the ASC X12 Standards for Electronic Data Interchange Technical Report Type 3 (TR3) and NOT a replacement for the standard TR3 for each transaction set. Based upon reporting circumstances, certain loops or data elements that are normally situational may become required. Some of these situational loops may not be included within the TCCG for a given transaction; however, requirements within TR3s must be followed when using different loops, segments and data elements. TR3 required information must be met even if it's not part of the TCCG. The TR3s can be obtained exclusively from the Washington Publishing Company by calling (800) 972-4334 or downloaded from their web site at www.wpc-edi.com.

TCCGs are intended for the technical staff of the external entities that will be responsible for the electronic transaction/file exchanges. TCCGs are available to TennCare registered Trading Partners to clarify the information on HIPAA-compliant electronic interfaces with TennCare. The purpose of the TCCG documents is to provide information necessary to submit accepted transactions to TennCare electronically.

Disclaimer: TennCare Companion Guides are intended to be technical documents describing the specific technical and procedural requirements for interfaces between TennCare and its trading partners. TCCGs do not supersede either the Managed Care Contractors (MCCs) contracts or the specific procedure manuals for various operational processes. Where there are conflicts between TCCGs and, either, the MCC contracts or operational procedure manuals, the contract or procedure manual will prevail. Substantial effort has been taken to minimize any such conflicts or errors; however, TennCare or its employees will not be liable or responsible for any errors or expenses resulting from the use of information in these documents. If you believe there is an error in any document, please notify TennCare EDI at EDI.TennCare@tn.gov.

Section 1.03 TennCare Introduction

TennCare is pleased to make available our current version of HIPAA Companion Guides. These documents were the culmination of a long process and represent a significant milestone in our ongoing effort to adhere to the HIPAA transaction set requirements and requirements of the Affordable Care Act (ACA) Section 1104. HIPAA and the ACA provide all healthcare entities a tremendous opportunity to realize many administrative and systemic benefits because it provides national standards of transaction and code sets for the electronic exchange of healthcare information. TennCare is committed to the implementation of all needed HIPAA transaction sets within the TennCare Management Information System (TCMIS).

HIPAA does not mandate the use of these transaction sets for the exchange of healthcare data except for certain Medicaid claims. Any provider may continue to submit paper claims and receive a paper remittance advice. However, if a provider elects to submit claims electronically and/or receive an electronic remittance advice, HIPAA does require the use of standard transactions and code sets. Currently, TennCare makes available to registered/credentialed providers downloadable electronic remittance advice transactions and PDF versions of the paper remittance advice via the Provider Data Management System (PDMS) Portal. Providers can request secondary account access if needed once the primary account access is established. Questions regarding the PDMS Portal should be directed to TennCare Provider Services at (800) 852-2683.

All comments, suggestions, and/or questions regarding TCCGs should be directed to:

TennCare EDI
Bureau of TennCare
310 Great Circle Road
Nashville, TN 37243
Email: EDI.TennCare@tn.gov

Submitters are requested to refrain from contacting our facility manager regarding any HIPAA issues or questions and either use the Provider Services or EDI information provided above.

Section 1.04 PPACA/ACA Section 1104 Overview

The Patient Protection and Affordable Care Act (PPACA), commonly called the Affordable Care Act (ACA), was enacted March 23, 2010. ACA Section 1104 requires the Secretary of the Department of Health and Human Services (HHS) to adopt and regularly update standards, implementation specifications, and operating rules for the electronic exchange and use of health information for the purposes of financial and administrative transactions. ACA Section 1104 also mandates that all HIPAA-covered

entities are required by Federal law to adopt CAQH CORE operating rules that improve the utilization of existing HIPAA transactions and reduce administrative costs. CORE Operating Rules Phase I and II for Eligibility and Claim Status HIPAA transactions have an established adoption deadline of July 1, 2011 and an effective date of January 1, 2013. CORE Operating Rule III for Electronic Fund Transfer (EFT) and Electronic Remittance Advice (ERA) transactions has an established adoption deadline of July 1, 2012 and an effective date of January 1, 2014. CORE Operating Rule IV for enrollment and referral authorization transactions has an established adoption deadline of July 1, 2014 and effective date of January 1, 2016.

Section 1.05 HIPAA Supported Transactions

HIPAA, the "Health Insurance Portability and Accountability Act", enacted on August 21, 1996 requires several provisions. One provision deals with the portability of health insurance coverage during a change in employment, and primarily affects employers and health insurers. Another provision often referred to as "Administrative Simplification", deals with the implementation of healthcare standards, of which transaction and code sets are but one part. The following HIPAA transaction sets are currently supported by TennCare:

(a) Eligibility Inquiry and Response: HIPAA mandates X12 V5010X279A1 – 270/271 Eligibility, Coverage or Benefit Inquiry and Information EDI Transactions for this purpose.

(b) Claim Status Inquiry and Response: HIPAA mandates X12 V5010X212 – 276/277 Claim Status Request and Information Status Notification EDI Transaction for this purpose.

(c) Referral Certification and Authorization: HIPAA mandates X12 V5010X217 – 278 Health Care Service Review EDI Transaction for this purpose. This transaction is supported but not currently used by businesses.

(d) Premium Payment and Remittance Advice: HIPAA mandates X12 V5010X218 – 820 Payment Order/Remittance Advice EDI Transaction for this purpose. This transaction is used between TennCare and its Managed Care Contractors (MCCs) only.

(e) Enrollment and Disenrollment: HIPAA mandates X12 V5010X220A1 – 834 Benefit Enrollment and Maintenance EDI Transaction for this purpose.

(f) Claim Payment and Remittance Advice: HIPAA mandates X12 V5010X221A1 – 835 Healthcare Claim Payment/Advice EDI Transaction for this purpose. Provider 835s for crossover and special waiver claims payment are available via the PDMS portal only.

(g) Claims and Encounters: HIPAA mandates the X12 V5010X223A2 – 837 Health Care Claim: Institutional, V5010X224A2 - 837 Health Care Claim: Dental, and V5010X222A1 - 837 Health Care Claim: Professional. HIPAA mandates NCPDP D.0 for interactive pharmacy transactions which are reported to TennCare using the NCPDP PAS 3.0 transaction. TennCare uses the 837s for fee-based claims and all non-pharmacy encounters. A TennCare encounter is a fully, post-adjudicated claim.

Claim attachments and updates for all transaction sets are actively being developed by standards workgroups for future implementation.

HIPAA also requires the standardization of code sets. Any coded field or data element contained in a HIPAA transaction must adhere to a national set of code set values, including medical services and diagnoses. As such, TennCare discontinued use of local codes in 2004, most notably the Level III HCPCS (procedure codes), which were specific to TennCare. TennCare currently only uses standard code set values.

Although TCCGs deal with only one aspect of the entire "Administrative Simplification" provision, it is worth noting that all covered entities (health plans, clearinghouses, and providers) and their business partners are required to adhere to all aspects of the provision.

Article II. Trading Partner Agreement and Supporting Documents

Section 2.01 General Overview

Each electronic submitter will be required to complete a trading partner agreement (TPA) and referenced attachments. Most EDI documents are available online at http://www.tn.gov/tenncare/topic/electronic-data-interchange. Others will be provided as part of forms processing. The TPA will be used to approve submitter identification information that is required on the HIPAA transactions. The first section of the TPA contains all of the legal requirements. The next sections are forms used to specify transaction and security arrangements.

Two copies of a completed TPA must be mailed to TennCare at the address above or a scanned image can be emailed to EDI.TennCare@tn.gov. After the TPA is reviewed, it will be signed and one copy returned to the originator.

Section 2.02 TennCare Electronic Data Interchange Request Form

The TennCare Electronic Data Interchange (EDI) Request Form is a supplemental part of the TPA. The EDI Request Form is completed by the entity and provides a summary of the information exchanged between the entity and TennCare. This form contains information concerning:

(a) Who is the contract entity?
(b) Who is authorized to add or change the data being provided or received or the users authorized to access the data?
(c) Who will actually submit the data, if different from the contracted entity?
(d) What type of data will be accessible to the entity (e.g., 834 files, encounter or claims files, provider reference files or 270/271 eligibility data)?
(e) How the data exchange will occur (e.g. SFTP or other)?
(f) What is the entity's current user ID, if available?
(g) Which transactions will generate a functional acknowledgement from the entity?

The TennCare Electronic Data Interchange (EDI) Request Form includes the 835 Healthcare Claim Payment/Advice EDI Transaction for selection. Note: **Registered providers are not required to submit an EDI Request Form just for the 835**. TennCare produces Provider 835 Remittance Advices, which are only available via the Web based PDMS (Provider Data Management System) Portal to the Provider. The Provider must be registered in PDMS for access. Provider Registration and credentialing information is available at http://www.tn.gov/tenncare/topic/provider-registration. A provider is not prohibited from sharing their logon credentials with the clearinghouse of their choice or requesting a secondary set of credentials but access is limited to registered TennCare healthcare related providers and groups with the proper credentials in our Provider Registration portal. Questions regarding the PDMS Portal should be directed to TennCare Provider Services at (800) 852-2683.

Section 2.03 TennCare User Security Agreement

The TennCare User Security Agreement outlines the responsibilities associated with access to TennCare data. All TennCare users in the entity authorized to access data using the connection to TennCare must sign that

they understand and will comply with the listed responsibilities. SFTP users will be provided an Acceptable Use Policy (AUP) that must be signed prior to access being granted. *Entities are responsible for the actions of their staff*. All users are expected to and will be required to comply with all Federal law, State of Tennessee law, and TennCare policies and procedures regarding data confidentiality, privacy, security, and user access.

Section 2.04 TennCare Remote Access Request Form

The Remote Access Request (RAR) form is required for SFTP access only and necessary as part of the TPA in order to assign a user ID.

Section 2.05 Additional Forms

The following forms are to be provided upon TPA approval as needed:

(a) Submitter Only Provider Application
(b) Business Associated Agreement (BAA)
(c) Fee-based Contract

Article III. EDI Services and Fees

Section 3.01 EDI Services

TennCare is a managed care program and all of our member's claims (837Is, 837Ps, 837Ds, NCPDP PAS3.0, NDPDP Batch 1.2 and their associated claims remittance information (835s) are processed by our MCCs. A listing of TennCare's health plans and their contact information is available online at http://www.tn.gov/tenncare/topic/providers-managed-care-organizations. Links to pharmacy and dental services contractor information can also be found to the left on this web page.

TennCare offers three options for eligibility verification for clearinghouses that service providers of TennCare's members. They are TN Online Services

(web access), 270/271 batch via SFTP and 270/271 real-time via direct SOAP connection.

TennCare has the Provider Data Management System (PDMS) web portal for registered/credentialed Providers that offers' eligibility verification, downloadable paper remittance advice (PDFs), and downloadable 835 transaction files. A provider is not prohibited from sharing their logon credentials with the clearinghouse of their choice but access is limited to registered TennCare healthcare related providers and groups with the proper credentials in our Provider Registration portal. Providers can request secondary credentialed access for themselves or entities that represent them as well once their primary account is established. Provider Registration information can be found at this link, http://www.tn.gov/tenncare/topic/provider-registration and further assistance can be received by contacting TennCare Provider Services at (800) 852-2683. TennCare Provider Services currently anticipate the registration and credentialing of providers to be within 10 business days.

Section 3.02 Fees

TennCare's three current Fee-based Contract options are as follows:

(a) TN Online Services

(i) Web access

(ii) 1 member at a time

(iii) $75 annual fee

(b) 270/271 Batch

(i) Via SFTP

(ii) 1 to 100,000 members per 270

(iii) One-time $2,500 set-up fee plus $0.02 per eligibility request

(iv) Average 271 response time is 45 minutes to 2 hours depending on volume

(c) 270/271 Real-time

(i) Direct SOAP connection

(ii) 1 member at a time

(iii) One-time $10,000 set-up fee plus $0.04 per eligibility request

(iv) Average 271 response time is approximately 0.15 seconds

Article IV. Technical Environment and Testing Considerations

Section 4.01 TennCare Communications Requirements

TennCare continues to evaluate and maintain current applicable methods of communications or upgrading as required with the most current and secure methods of communicating within the TCMIS. The primary method of connecting to the TennCare network is by going from the Internet through a Juniper Virtual Private Network (JVPN) tunnel to a secure FTP server. There are two types of JVPN connections available:

(a) *Software-to-Hardware*. JVPN client software is installed and configured on every machine at the client that requires SFTP access.

(b) *Hardware-to-Hardware*. The client's network is interfaced with the TennCare server allowing on-demand access to the SFTP server. This access is limited to large volume contractors only.

Detailed JVPN requirements can be obtained by contacting TennCare. In general, these requirements include network interface card or modem, working Internet connection with a firewall, and installed JVPN Client Software.

Section 4.02 File Encryption Procedures

Encryption is handled automatically as part of the creation of the JVPN tunnel. The JVPN client software on the user's computer or system will automatically de-encrypt the data after it reaches the user's system. All files and data that pass through the JVPN tunnel are encrypted using at least a 256-bit algorithm. All TennCare handled data is encrypted at rest and during transport at all times.

Section 4.03 File and Directory Naming Conventions

The directory structure and file naming standards on the SFTP server are designed to provide logical access to all files, ease troubleshooting searches, and simplified security for account set ups and maintenance. TennCare's SFTP naming conventions follow.

Filenames for most HIPAA transactions will be of the format

AAAABBBYYMMDDSS.EEE

Where **AAAA** is transaction type,
BBB is the last 3-bytes of the assigned trading partner ID number,
YYMMDD is transmission date,
SS is transmission sequence (starting at 01), and

EEE is file format (zip, gz, tar, etc.).

The **AAAA** values reflect the standard transaction type being transmitted as follows:

receive	**s**end	**u**nsolicited	**d**ental	**i**nstitutional	**p**rofessional
r270	s271	r271	d837	i837	p837
r276	s277	s271d			
r278	s820	s271u			
r834	s834				
r999	s999				

For example, i837ABC16090401.zip is the first institutional 837 from trading partner ABC sent on September 4, 2016 and the file is in a zip format. For the acknowledgement transaction, the second node contains the name of the transaction being acknowledged. See section 6.01 below. For the 271 response, the file is named after the 270 request transaction changing "r270" to "s271" for ease of visual re-association by the submitter.

MCC encounter transactions are named following the naming standard as established in the TennCare Encounter Claims naming standard policy. TennCare Encounter policies are available on the TennCare website under Policy & Guidelines, Information Systems Policies menu selection at http://tennessee.gov/tenncare/topic/information-systems-policies. Or directly download the Encounter File Naming Standard document at http://tennessee.gov/assets/entities/tenncare/attachments/encounterdatapolicyworkgroup.pdf.

Naming standards for non-X12 transmissions will be provided upon completion of the TPA to those approved for a given transaction. *Note that TennCare expects all files to be compressed with internal filename equal to the external filename with a .txt, .dat, etc. extension.*

Section 4.04 Multiple Transactions within a File

TennCare does not allow multiple transaction types to be submitted within a single interchange submission (ISA-ISE). While the X12 standards allow for multiple transaction set types such as an 837I, 837P, and 834 to be submitted within an ISA-IEA, TennCare does not support transaction bundling within a file. It is thought that this limitation provides for a "cleaner" processing environment. Multiple ISA-IEA sets within a single file are supported but not recommended.

Section 4.05 Size of Transmissions/Batches

Fee-For-Service transmission sizes are limited based upon the number of Segments/Records allowed by TR3 standards. Standards for the maximum file size of each transaction set are specified in the appropriate TR3 or its authorized addenda.

X12 transmission sizes are based upon TennCare file transfer limits developed during systems testing. These limits are generally larger than the recommendations in TR3s. For X12 837 transactions, the limit is 5,000 claims per ST to SE batch with a 250,000 claim limit per file. For 270 and 271 transactions, TennCare has imposed a limit of 100,000 member records per file due to response processing time limitations. For the 834 and 835 we have no ST-SE or ISA-IEA limits. Due to the construct of the 820 transaction the limit is 999,999 ENT records per ST-SE in the 820. There is no limit on the NCPDP PAS 3.0 transaction file sizes other than the uncompressed file must be less than 1 GB.

Section 4.06 Complete Transmission Check

All transactions are checked to ensure that the transmission is complete. The transaction header and footer must balance before an ISA-IEA is processed.

Section 4.07 Strategic National Implementation Process (SNIP) Test Types

TennCare requires each prospective electronic data interchange (EDI) submitter to be tested and approved before HIPAA transactions will be processed in production. TennCare will conduct the required testing with a submitter via test file(s) from the submitter to TennCare in one of our test environments. The Workgroup for Electronic Data Interchange (WEDI), through a collaborative healthcare industry effort called the Strategic National Implementation Process (SNIP), developed seven types of transaction testing:

1) Integrity Test: Testing of the EDI file for valid segments, segment order, element attributes, testing for numeric values in numeric data elements, validation of X12 syntax, and compliance with X12 rules. This will validate the basic level integrity of the EDI submission.

2) Requirement Test: Testing for TR3 specific syntax requirements, such as repeat counts, used and not used codes, elements and segments, required or intra-segment situational data elements. Testing for non-medical code sets as laid out in the TR3. Values noted in the TR3 via an X12 code list or table.

3) Balance Test: Testing the transaction for balanced field totals, financial balancing of claims or remittance advice, and balancing of summary fields, if appropriate.

4) Situational Test: Testing of specific inter-segment situations described in the TR3, including the validation of situational fields based on rules present in the TR3 for loops, segments, and data elements.

5) External Code Set Test: Testing for valid TR3 specific code set values. This type will not only validate the code sets but also make sure the usage is appropriate for any particular transaction.

6) Specialty of Line of Business Test: Testing to ensure that the segments and data elements required for certain healthcare services are present and correctly formatted according to the TR3.

7) Trading Partner Requirements Test: Testing to ensure that trading partner specific requirements are implemented. TennCare does enforce multiple SNIP 7 edits for most claims and select other transactions.

Testing for TennCare is only required for the transactions that an organization is approved to conduct with TennCare. Separate testing as appropriate will be required for each transaction type. TennCare is not interested in testing on transactions that are not appropriate for the Business Associate relationship. Once testing is validated, the submitter is placed into production for the approved transaction.

Section 4.08 Balancing Data Elements

TennCare will utilize balancing requirements that can be derived from the

transaction TR3. All financial amount fields must be balanced at all levels available within the transaction set. The number of transactions in the header and footer must equal and be the same as the number of transactions in the file. TennCare has custom SNIP 7 edits in place for enforcement of balancing requirements where standard SNIP 1-7 edits do not exist. A listing of custom SNIP 7 edits is provided to an approved trading partner for any impacted transaction.

Article V. Testing Procedures

Section 5.01 Testing Requirements

TennCare will require testing with all of its trading partners before a transaction is placed into production. TennCare offers testing with its trading partners as a means to test TCCG requirements and to prove production readiness. Third party certification is not required or accepted by TennCare as a substitute for pre-production testing with Tenncare. Note, TennCare maintains a third-party certification of its capability to produce compliant transactions.

TennCare reserves the right to discontinue any testing with any submitter if TennCare determines that errors, which should have been corrected by the submitter, are present. TennCare offers full production volume testing, when necessary or desired.

TennCare expects each individual trading partner to be responsible for ensuring that its transactions are compliant. Compliance includes both the HIPAA mandates and TennCare Trading Partner requirements contained in the TCCGs. Compliance testing should include the internal validation of all used transaction sets by the submitting trading partner.

Section 5.02 Test Data

TennCare believes that, where possible, using "real" data will enhance the overall value of the compliance testing process. However, if the covered entity elects to do so it must ensure that it remains in compliance with all Federal and State privacy regulations. In particular, TennCare expects that Patient Identifiable Information will be encrypted or eliminated from tests submitted to the certification testing system unless the testing system is in compliance with all HIPAA regulations concerning security, privacy, and business associate agreements.

Article VI. Acknowledgment Processes

Section 6.01 Overview of Acknowledgment Processes

Acknowledgment transactions let the sender know that the receiver received their transactions and that the transactions have been accepted with no errors, accepted with errors, or rejected. The two types of Acknowledgment Transactions used by TennCare are the:

(a) Interchange (TA1) Acknowledgment
(b) Functional Acknowledgment Transaction Set (999)

In addition to the standard TA1 and 999, TennCare creates an outbound acknowledgement package for all batch X12 transactions. This package is called the "sedi" (Send EDI) package. The package contains the TA1, 999, an HTML error report, an HTML summary report and, if applicable, a bad file. The bad file contains all rejected transactions. The second node of the "sedi" package filename contains the name of the originally submitted transaction file. For example, sediABC17021502.r834ABC17021401.zip would be a response to an inbound 834 from trading partner ABC on February 14, 2017 that was processed on February 15, 2017.

Section 6.02 TennCare Requirements

(a) TennCare uses the 999 and TA1 transactions within the "sedi" package to acknowledge all X12 files received by TennCare.

(b) A trading partner may elect to send TennCare an acknowledgement on any or all files. These acknowledgements should be listed on the EDI Request Form.

Section 6.03 Rejected Transmissions and Transactions

The process for handling rejected transactions and transmissions will vary based on the error(s) causing the rejection.

(a) Interchanges or functional groups may be completely rejected for TR3 format violations.

(b) Individual transactions or transaction sets within a functional group/interchange can be rejected.

(c) Rejection of encounter data will be done at the claim level or transaction set level dependent upon the error type.

Numerous edits will be performed on each transaction processed. Each of these edits has a severity level associated with it that in conjunction with the number of errors will determine accept/reject status at all levels listed above.